Jim Bugel
Assistant Vice President
Federal Regulatory

AT&T Services, Inc.
1120 20TH Street, NW
Suite 1000
Washington, DC 20036

T: 202.457.2052
F: 202.457.2008
Jb2229@att.com

October 30, 2009

VIA ELECTRONIC SUBMISSION

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, D.C. 20554

Re: National Broadband Plan Proceedings Docket No. 09-51

Dear Ms. Dortch:

Pursuant to the letter dated October 9, 2009, from Jennifer Manner, Deputy Chief, Public Safety Homeland Security Bureau, attached please find John Nagengast's responses to the follow-up questions from the October 2, 2009 FCC Cyber Security Workshop.

If you have any other questions, please feel free to call me at 202.457.2052.

Sincerely,

/s/Jim Bugel
AT&T Services, Inc.

Attachment

John C. Nagengast
Executive Director

AT&T Government Solutions
7125 Columbia Gateway Drive
Suite 210
Columbia, MD 21046

443.259.8366 Phone
jn2317@att.com E-mail

October 30, 2009

Ms. Jennifer A. Manner
Deputy Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission
Washington, DC 20554

Re: National Broadband Plan Proceedings Docket No. 09-51

Dear Ms. Manner:

The following provides our response to your October 9, 2009, letter. Our answers to the specific questions in your letter are contained following the body of this letter.

Cyber security is an extremely complex challenge with many and varied dimensions. It involves policy and social issues, as well as the ever dynamic technology and architecture of the global digital infrastructure. Cyber security involves the many varieties of end user devices and the applications and software they employ, the access methods that connect these devices to the global infrastructure, the protocols which allow these devices and applications to communicate with each other, the content which users and/or their applications want to access, and the core infrastructure itself - including such enablers as the Domain Name System.

AT&T has implemented an extensive capability within our core network infrastructure to detect and mitigate cyber attacks against our infrastructure and our customers. We offer an extensive set of managed security services to our business and government customers, including advanced VPN capabilities, network-based firewalls, intrusion detection, and DDOS mitigation, and look to expand this capability into the consumer space in the future. Via the GSA Networx contract, we are introducing Managed Trusted Internet Protection Service to our government customer base, which represents a significant step forward in managed, network-based cyber security services. We believe providing advanced cyber security services to our customers is a major business imperative, and is an integral part of our strategy to provide secure, reliable and resilient networking capabilities and on-demand applications and content via any access medium to our global customer base.

It was a pleasure to participate in the Cyber Security Workshop held on September 30, 2009, and

we look forward to further engagement with the FCC on this important topic.

Sincerely,

/s/ John C. Nagengast
Executive Director, Strategic Initiatives
AT&T Government Solutions

Questions and Answers

Q. What would motivate more network providers to adopt approaches to improve security when effectiveness depends on what other providers do, as might be the case with authentication, routing security, and DNS security? Are there policies that the U.S. Government should consider in the broadband plan to encourage this?

A. Given the current environment of rapidly increasing cyber threats, network providers are universally interested in improving cyber security, both individually and collectively. Commercial network providers are themselves targets of every type of cyber attack. A provider's network does not operate smoothly if the infrastructure is compromised; an operator suffering outages will see customers taking their business elsewhere. Likewise, if sensitive information is compromised, the impacted customers will move to other suppliers. Simply put, cyber security is a business imperative today for service providers.

AT&T is on record with plans to invest $18 billion this year to improve and expand our global infrastructure, including its reliability, resiliency, and security. These investments are driven by business objectives - meeting customer demands and improving competitive positioning in the marketplace, and are focused on achieving definable results commensurate to the substantial investment made.

The government should avoid any action that might discourage continued investment by, and competition among, service providers to make their technology, systems, and networks more secure. A regulatory and standards-based approach, for example, could never keep up with the dynamics of the technology and the rapid evolution of global threats, and would tend to stifle innovation.

In the case of collective improvements in security referenced in the question - authentication, routing security, and DNS security - viable, cost effective solutions to achieve measurable improvements in security are not readily available. For example, DNSSEC protects against a particular class of attack - cache poisoning - but does nothing to protect against the broader class of DNS amplification attacks, and actually makes the DNS infrastructure more vulnerable to these types of attacks due to the increased computational cycles required to process a DNSSEC transaction. Also, the recent disruption of Internet Access to Sweden (.sw) was caused by a simple typing error in doing a TLD update to the .sw zone, but the recovery was made more complicated and time consuming by DNSSEC.

Further, the network providers are only one part of the DNS. ICANN, IANA, and the Domain Name Registrars, such as Verisign, Neustar, etc., manage and operate the core of the DNS Infrastructure. Likewise, no immediate ways to improve the fundamental security of interdomain routing have been identified. The IETF has developed an authentication extension of BGP, referred to as S-BGP, but it does little to counter the most prevalent threats to BGP-based peering while adding complexity and overhead.

The most helpful role the U.S. Government can play in making collective improvements in interdomain security is to expand investment in research and development to provide effective and efficient solutions to the current vulnerabilities, working in concert with the key stakeholders, including ICANN and the IETF, the network hardware and software providers, and the network service providers. Without these technical solutions, governmental policies will do little to effect change.

Q. With respect to information sharing about outcomes and results, what incentives are needed to encourage service providers to report more data about the occurrence and resolution of cyber security incidents to their customers, the FCC, other government or security-focused agencies, and competitive service providers?

A. AT&T routinely provides cyber status information and alerting to business enterprise customers through Service Level Agreements and our AT&T Internet Protect (SM) service. We are currently exploring how to better engage small business and consumer customers on cyber security, including warnings and advisories along with assistance in remediation.

Service Providers will be incentivized to share cyber security information with government entities if:

1. They can be assured that the information, which is proprietary, will be protected;

2. There are clear and tangible benefits to doing so in protecting their individual networks and customers; and

3. There is a clear legal framework for conducting the sharing, including with respect to civil liability, anti-trust protection, inter-agency sharing, and treatment of requests from the public for information under FOIA.

The government should avoid creating new reporting requirements and mechanisms where such requirements essentially already exist. Rather, stakeholders should collectively work to leverage and consolidate existing efforts by government and industry, and expand the best of what is out there. For example, AT&T is actively engaged with a number US government and government-sponsored information initiatives and organizations to enhance our nation's cyber security. These include, but are not limited to:

- Computer Emergency Response Team/Coordination Center (CERT/CC)

- Forum of Incident Response and Security Teams (FIRST)
- National Coordinating Center for Telecommunications (NCC)
- Network Reliability and Interoperability Council (NRIC)
- Communications - Information Sharing and Analysis Center (Communications-ISAC)
- Network Reliability Steering Committee (NRSC)
- The National Telecommunications and Information Administration (NTIA)
- National Communications System (NCS)
- National Security Telecommunications Advisory Committee (NSTAC)
- Federal Bureau of Investigation's InfraGard
- U.S. Secret Service (USSS) Cyber Crimes Task Force
- National Security Information Exchange (NSIE)
- Shared High Frequency Radio Resources (SHARES) Program
- Communications Sector Coordinating Council (SCC)
- Telecommunications Service Priority (TSP) Oversight Committee.

To provide a coherent, consolidated framework for cyber incident reporting and response coordination, AT&T supports the recommendations in the recent NSTAC Report to the President on Cyber Security Collaboration, dated 21 May 2009. This report recommends the establishment of a government-sponsored Joint Collaboration Center, initially building on the existing capabilities of the Network Coordinating Center and U.S. CERT, sponsored by DHS. The report includes discussion of all of the issues which need to be addressed in providing this capability.

Q. Should there be a mandatory threshold of affected systems or networks by cyber incidents at which providers must report information to the FCC and other government agencies such as US-CERT and the National Coordination Center (NCC)?

A. Mandatory thresholds for reporting will be difficult to define in something as dynamic and amorphous as cyber security. We believe a voluntary approach driven by clear incentives and benefits to the entity providing the data (as discussed above) is a much more practical approach.

This would include the capability to better coordinate mitigation and response activities in timely fashion.

Q. Should US-CERT, the NCC and any other government-supported entity that receives such information, adhere to confidentiality agreements with commercial providers to allay concerns about the disclosure of competitive market data and proprietary information?

A. As mentioned above, protection of proprietary and sensitive information is an essential component of any sharing relationship between service providers and government. A clear legal framework governing all aspects of the relationship - including what gets shared, and what the government entity can do with the shared information and how it will be protected - are fundamental to a successful and beneficial relationship.

Q. What could ISPs do to offer their subscribers more security to protect end users intellectual property and data integrity and compromise from cyber thieves that may gain access to this information using key loggers, IP masking or other virtual means to access end users data?

A. AT&T currently offers a comprehensive set of managed security services to large business enterprise customers, and we are now expanding this service into the small and medium-sized business area. These services include authentication and encryption for protecting data at rest (stored data) and data in transit (e-mail, file transfers, etc.) Other service providers also offer a variety of managed security services. In cases where subscribers do not take advantage of such services, they may not fully understand the threats and vulnerabilities, or they may believe it is less expensive to attempt to manage cyber security on their own. Expanding cyber security education and awareness, along with demonstrating the advantages of a comprehensive, network-based approach to security, would help to create market demand for, and greater utilization of, these services.

Q. Would it be possible to implement hashing, 256 or 512 Bit encryption, sha 64+1, RSA Token Authentication to ensure the protection of the end users data?

A. Authentication and encryption are both essential components of a comprehensive cyber security strategy. Authentication of transactions along with encryption of data both at rest and in transit can help to protect end-user data from unauthorized access or modification. NIST has done an excellent job in developing standards to support authentication and encryption, and many commercial products are available that support these standards. The missing link to deploying authentication and encryption on a widespread basis is a scalable and trustworthy identity management system. This provides the foundation for comprehensive application of authentication and encryption services across the full spectrum of applications. NSTAC recently produced a Report to the President on Identity Management, dated 21 May 2009, which provides a comprehensive set of recommendations on establishing a national identity management strategy through a broad and enduring government and private sector partnership.

Also, while encryption and authentication provide powerful tools, they alone do not completely assure the protection of data. By gaining surreptitious root access to an end-user platform or server, an intruder can by-pass authentication/access control mechanisms and capture and exfiltrate data "in the red" while it has been unencrypted for viewing or processing. That is why authentication and encryption should be used as *part* of a comprehensive, network-based cyber security program.

Q. How have more complicated supply chains from diverse sources, including from outside the United States, introduced vulnerabilities into information and/or network technologies and affected cyber security? Are commercial service providers adequately addressing any such vulnerabilities and, if not, what can be done to better address these concerns?

A. Supply chain security is one of the more challenging aspects of cyber security, given the globalization of the technology market. Clearly this is where expanded cooperation between the private sector and government is necessary, particularly where a sophisticated nation-state adversary is assumed. Given the widespread globalization of development and the outsourcing of manufacturing, the only viable approach to protecting the core network is to assume that no hardware and software components can be trusted, and to monitor their behavior to identify malicious activity.

Q. What ways can state and federal agencies and organizations work together to develop a uniform set of standards for identifying, analyzing, resolving, and reporting cyber attack incidents to their customers, the FCC, other government or security-focused agencies, and competitive service providers?

A. This is a complex subject with many dimensions. As mentioned earlier, the development of standards for even the reporting of cyber attack incidents is problematic given the wide spectrum of possible attack scenarios and the dynamic nature of cyber threats. We recommend that a dialog on this topic start with a definition of the operational objectives and the conceptual development of an operational model to fulfill these objectives. We would again point out that AT&T supports the recent NSTAC recommendations on this topic in its 21 May 2009 report.

Q. What are the processes that are being put in place to take into consideration the convergence of technologies and security threats at the same time?

A. First and foremost, cyber security is an extremely complex challenge with many and varied dimensions. It involves policy and social issues, as well as the ever dynamic technology and architecture of the global digital infrastructure. "Convergence" as that term is commonly used is perhaps a misnomer -- innovation enables some service providers to place the many and varied applications they support onto a common IP backbone, but the applications, the access media, and the end-platforms are all becoming more diverse and complex. The clear advantage of convergence with respect to cyber security is the ability of a Service Provider to detect malicious activity in the common IP backbone, independent of the particular application, access medium, or end-platform, and to block the malicious activity in the core where possible.

Q. The panelists expressed concern that infrastructure security problems often result from end users not using security applications to protect their home computers. What additional steps or educational tools are needed to make people aware of the need to secure their computers?

A, While we view expanding consumer awareness and education on cyber security to be essential, particularly with respect to such non-technical threats as phishing, even the most sophisticated users are challenged by the many rapidly changing cyber threats and the inherent vulnerabilities in the underlying technology and platforms they employ, whether a desktop, laptop, or wireless/mobile device. To make a significant improvement against technical threats in the end user device, the technology providers must make security and security applications a seamless part of the platforms they provide for both consumer and business users. These security applications must be properly configured and constantly updated to maintain their relevance, and this can only be done through professional security management services.

We believe that the service providers are in a unique position to provide these management services, given their real-time awareness of emerging threats via the global digital infrastructure. Thus, education efforts should focus on increasing consumer awareness of the need for greater security in the products they buy and, thereby, stimulating demand for the managed security services that are available to them.

End of Questions and Answers
